UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/809,532	03/26/2004	Akira Yaegashi	SON-2960	7528

23353 7590 10/24/2008
RADER FISHMAN & GRAUER PLLC
LION BUILDING
1233 20TH STREET N.W., SUITE 501
WASHINGTON, DC 20036

EXAMINER	
CUTLER, ALBERT H	

ART UNIT	PAPER NUMBER
2622	

MAIL DATE	DELIVERY MODE
10/24/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/809,532	YAEGASHI, AKIRA	
	Examiner	Art Unit	
	ALBERT H. CUTLER	2622	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 September 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4 and 14-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *18-21* is/are allowed.

6)☒ Claim(s) *1-4,14-17, and 22-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is responsive to communication filed on September 16, 2008.

Response to Arguments

2. Applicant's arguments, see pages 9-16, filed September 16, 2008, with respect to the rejection(s) of claim(s) 1-4 and 18-21 under 35 U.S.C. 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection in claims 1-4 is made in view of Nakamura (US 5,159,633).

3. Applicant's arguments with respect to the rejection of claims 14-17 and 22-24 have been fully considered but they are not persuasive.

4. Applicant alleges that for the reasons stated above claims 14-17 and 22-24 also overcome Hamilton and Read. However, claims 14-17 and 22-24 are clearly different in scope and content from claim 1. 37 CFR 1.111(b) requires applicant to distinctly and specifically point out the supposed errors in the Office's action and reply to every ground of objection and rejection in the Office action. The reply must present arguments pointing out the specific distinction believed to render the claims patentable over any applied references (See MPEP § 2141 IV).

5. Therefore, the rejection of claims 14-17 and 22-24 is maintained by the Examiner.

Claim Objections

6. Claim 18 is objected to because of the following informalities: Lack of clarity and precision.

Claim 18 recites "**a** image transmission system". It appears that claim 18 should recite "**an** image transmission system". The Examiner will interpret claim 18 to read "**an** image transmission system". Appropriate correction is required.

Claim 18 also recites "requesting that the authentication server authenticate a user and authenticate that a user can access the **image pickup device**". However, no "image pickup **device**" has been previously defined. Upon further examination, it appears that claim 18 should read "requesting that the authentication server authenticate a user and authenticate that a user can access the image pickup **apparatus**". The Examiner will interpret claim 18 to read "requesting that the authentication server authenticate a user and authenticate that a user can access the image pickup **apparatus**". Appropriate correction is required.

Claim 18 also recites "decrypting images received from the **image pickup device** using the decryption key". However, no "image pickup **device**" has been previously defined. Upon further examination, it appears that claim 18 should read "decrypting images received from the image pickup **apparatus** using the decryption key". The Examiner will interpret claim 18 to read "decrypting images received from the image pickup **apparatus** using the decryption key". Appropriate correction is required.

7. Claim 19 is objected to because of the following informalities: Lack of clarity and precision.

Claim 19 recites, "The method of claim 18". However, claim 18 is directed to "A computer program, stored on a computer readable medium, for making a computer

perform the steps of". Upon further examination is appears that claims 19 should recite, "The computer program of claim 18, making the computer perform the further step of", or something of similar nature. The Examiner will interpret claim 19 to read, "The computer program of claim 18, making the computer perform the further step of". Appropriate correction is required.

Claim 19 also recites "accessing the authentication server from **a** viewing apparatus". However, a viewing apparatus has been previously defined in claim 18. Upon further examination it appears that claim 19 should recite "accessing the authentication server from **the** viewing apparatus". The Examiner will interpret claim 19 to read "accessing the authentication server from **the** viewing apparatus". Appropriate correction is required.

8. Claim 20 is objected to because of the following informalities: Lack of clarity and precision.

Claim 20 recites "authenticate **an** image pickup **device** accessible by the user". An image pickup **apparatus** has been previously defined in claim 20. Upon further examination it appears that claim 20 should recite "authenticate **the** image pickup **apparatus** accessible by the user". The Examiner will interpret claim 20 to recite "authenticate **the** image pickup **apparatus** accessible by the user". Appropriate correction is required.

Claim 20 also recites "decrypting the images received from the image pickup **device** using the decryption key". However, no "image pickup **device**" has been

previously defined. Upon further examination, it appears that claim 18 should read "decrypting the images received from the image pickup **apparatus** using the decryption key". The Examiner will interpret claim 18 to read "decrypting the images received from the image pickup **apparatus** using the decryption key". Appropriate correction is required.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. The factual inquiries set forth in *Graham* **v.** *John Deere Co.,* 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

11. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nakamura (US 5,159,633) in view of Hamilton (US 2002/0118837).

Consider claim 4, Nakamura teaches:

An image transmission system for transmitting an image via a network (see figures 1A and 1B), said image transmission system comprising:

one image pickup apparatus (first terminal, 1) having an encrypting function for encrypting a picked-up image for transmission to said network (The first terminal (1) is used for encrypting and transmitting real-time communication type information along a transmission path (3), column 4, lines 3-8. The image pickup apparatus includes a camera (106a) for picking up images for transmission, column 1, lines 5-9, column 4, lines 29-32. The images are transmitted in "an on-line manner", column 5, lines 40-52.);

a key generating apparatus for generating, for each said image pickup apparatus, an encryption key for said image pickup apparatus to encrypt the image and a decryption key (Images are encrypted in the image pickup apparatus (1) and decrypted in a viewing apparatus (2) using a generated "secret key", column 6, lines 11-16, lines 37-40. The encryption key is stored in a magnetic storage device (101) in the image pickup apparatus (1), column 6, lines 47-54, and transmitted to the viewing apparatus (2), column 9, lines 14-29. The secret keys are used to configure random number generators (109, 209) for encryption and decryption.); and

a viewing apparatus (second terminal, 2), having a decrypting function for decrypting said encrypted image using said decryption key, for communicating with said image pickup device, and for viewing the image transmitted via said network from said image pickup apparatus to said viewing apparatus (The viewing apparatus (2) comprises a CRT (206a) for displaying received image data, column 4, lines 61-66. Images are decrypted in a viewing apparatus (2) using a generated "secret key", column

6, lines 11-16, lines 37-40. The viewing apparatus (2) communicates with the image pickup apparatus (1) by requesting image data, column 6, lines 7-16. The viewing apparatus (2) decrypts encrypted image data using a key that is the same as the encryption key, which key is received from the image pickup apparatus, column 6, lines 47-69, column 9, lines 14-54.).

However, Nakamura does not explicitly teach that each image pickup device has a unique identifying number, or of a removable recording medium for recording said decryption key and the identifying number of said image pickup apparatus in association with each other.

Hamilton is similar to Nakamura in that Hamilton teaches (see figures 1 and 2) transmitting an encrypted image (28) obtained from a camera (20) via a network (see paragraphs 0055-0056). Hamilton also similarly teaches of decrypting the image at a receiving device using a decryption key (paragraph 0057).

However, in addition to the teachings of Nakamura, Hamilton teaches that each camera has an identifier, and that said identifier is a unique identifying number (serial number, 22, figure 1). Hamilton also teaches a removable recording medium for recording said decryption key and the identifying number of said image pickup apparatus in association with each other (The key(20) and the serial number(22) may be communicated from the retailer or manufacturer(i.e. the key generating apparatus) to an authorization center (i.e. image receiving device) by traditional hard copy methods (i.e. via a removable recording medium), paragraph 0079.). Hamilton also teaches that the image receiving device ("authorization center") is connected with the recording

medium (The authorization center can receive a "hard copy" of the key, paragraph 0079. This key is used for image decryption, paragraph 0057. Because the key is in hard copy form, it would have to be connected with the image receiving device.).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to have the camera taught by Nakamura comprise a unique identifying number as taught by Hamilton, and have the decryption key taught by Nakamura recorded on a recording medium as taught by Hamilton for the benefit of ensuring that the images obtained at the viewer are images from the specific image capture device (Hamilton, paragraph 0005).

12. Claims 1, 2 and 3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nakamura (US 5,159,633) in view of Hamilton (US 2002/0118837) and Read (US 2004/0066456).

Consider claim 1, Nakamura teaches:

An image transmission system for transmitting an image via a network (see figures 1A and 1B), said image transmission system comprising:

one image pickup apparatus (first terminal, 1) having an encrypting function for encrypting a picked-up image for transmission to said network (The first terminal (1) is used for encrypting and transmitting real-time communication type information along a transmission path (3), column 4, lines 3-8. The image pickup apparatus includes a

camera (106a) for picking up images for transmission, column 1, lines 5-9, column 4, lines 29-32. The images are transmitted in "an on-line manner", column 5, lines 40-52.);

a key generating apparatus for generating, for each said image pickup apparatus, an encryption key for encrypting said image and a decryption key for decrypting said encrypted image (Images are encrypted in the image pickup apparatus (1) and decrypted in a viewing apparatus (2) using a generated "secret key", column 6, lines 11-16, lines 37-40. The encryption key is stored in a magnetic storage device (101) in the image pickup apparatus (1), column 6, lines 47-54, and transmitted to the viewing apparatus (2), column 9, lines 14-29. The secret keys are used to configure random number generators (109, 209) for encryption and decryption.); and

a viewing apparatus (second terminal, 2), having a decrypting function for decrypting said encrypted image using said decryption key, for communicating with said image pickup device, and for viewing the image transmitted via said network from said image pickup apparatus to said viewing apparatus (The viewing apparatus (2) comprises a CRT (206a) for displaying received image data, column 4, lines 61-66. Images are decrypted in a viewing apparatus (2) using a generated "secret key", column 6, lines 11-16, lines 37-40. The viewing apparatus (2) communicates with the image pickup apparatus (1) by requesting image data, column 6, lines 7-16. The viewing apparatus (2) decrypts encrypted image data using a key that is the same as the encryption key, which key is received from the image pickup apparatus, column 6, lines 47-69, column 9, lines 14-54.).

However, Nakamura does not explicitly teach that each image pickup device has a unique identifying number, or of a removable recording medium for recording said decryption key and the identifying number of said image pickup apparatus in association with each other.

Hamilton is similar to Nakamura in that Hamilton teaches (see figures 1 and 2) transmitting an encrypted image (28) obtained from a camera (20) via a network (see paragraphs 0055-0056). Hamilton also similarly teaches of decrypting the image at a receiving device using a decryption key (paragraph 0057).

However, in addition to the teachings of Nakamura, Hamilton teaches that each camera has an identifier, and that said identifier is a unique identifying number (serial number, 22, figure 1). Hamilton also teaches a removable recording medium for recording said decryption key and the identifying number of said image pickup apparatus in association with each other (The key(20) and the serial number(22) may be communicated from the retailer or manufacturer(i.e. the key generating apparatus) to an authorization center (i.e. image receiving device) by traditional hard copy methods (i.e. via a removable recording medium), paragraph 0079.). Hamilton also teaches that the image receiving device ("authorization center") is connected with the recording medium (The authorization center can receive a "hard copy" of the key, paragraph 0079. This key is used for image decryption, paragraph 0057. Because the key is in hard copy form, it would have to be connected with the image receiving device.).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to have the camera taught by Nakamura comprise a unique

identifying number as taught by Hamilton, and have the decryption key taught by Nakamura recorded on a recording medium as taught by Hamilton for the benefit of ensuring that the images obtained at the viewer are images from the specific image capture device (Hamilton, paragraph 0005).

However, the combination of Nakamura and Hamilton does not explicitly teach an authenticating server for authenticating said image pickup apparatus accessible from said viewing apparatus.

Read is similar to Nakamura and Hamilton in that Read teaches an image transmission system (figure 1) for transmitting an image via a network (internet, 102), said image transmission system (figure 1) comprising one or a plurality of image pickup apparatus (104) each having a unique identifier (Cameras have unique identifiers so that a user can be permitted to or restricted from viewing certain cameras, paragraph 0036.).

However, in addition to the teachings of Nakamura and Hamilton, Read teaches an authenticating server (central server, 108) for authenticating said image pickup apparatus accessible from a viewing apparatus (The authenticating server (108) is accessible from a viewing apparatus (110, figure 1), and uses log-in/password security functions to authenticate that an image pickup apparatus is accessible by a viewing apparatus, paragraph 0024. If the viewer is authorized, then images received from the image capture device are immediately forwarded to the viewer, paragraph 0033.).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to include an authenticating server as taught by Read in the

image transmission system taught by the combination of Nakamura and Hamilton for the benefit of increasing security.

Consider claim 2, Nakamura teaches:

An image transmission system for transmitting an image via a network (see figures 1A and 1B), said image transmission system comprising:

one image pickup apparatus (first terminal, 1) (The first terminal (1) is used for encrypting and transmitting real-time communication type information along a transmission path (3), column 4, lines 3-8. The image pickup apparatus includes a camera (106a) for picking up images for transmission, column 1, lines 5-9, column 4, lines 29-32. The images are transmitted in "an on-line manner", column 5, lines 40-52.);

a key generating apparatus for encrypting an image picked up by said image pickup apparatus and transmitting the image to said network, and generating a decryption key for decrypting said encrypted image (Images are encrypted in the image pickup apparatus (1) and decrypted in a viewing apparatus (2) using a generated "secret key", column 6, lines 11-16, lines 37-40. The encryption key is stored in a magnetic storage device (101) in the image pickup apparatus (1), column 6, lines 47-54, and transmitted to the viewing apparatus (2), column 9, lines 14-29. The secret keys are used to configure random number generators (109, 209) for encryption and decryption. The image pickup apparatus acts as a key generating apparatus.); and

a viewing apparatus (second terminal, 2), having a decrypting function for decrypting said encrypted image using said decryption key, for communicating with said

image pickup device, and for viewing the image transmitted via said network from said image pickup apparatus to said viewing apparatus (The viewing apparatus (2) comprises a CRT (206a) for displaying received image data, column 4, lines 61-66. Images are decrypted in a viewing apparatus (2) using a generated "secret key", column 6, lines 11-16, lines 37-40. The viewing apparatus (2) communicates with the image pickup apparatus (1) by requesting image data, column 6, lines 7-16. The viewing apparatus (2) decrypts encrypted image data using a key that is the same as the encryption key, which key is received from the image pickup apparatus, column 6, lines 47-69, column 9, lines 14-54.).

However, Nakamura does not explicitly teach that each image pickup device has a unique identifying number, or of a removable recording medium for recording said decryption key and the identifying number of said image pickup apparatus in association with each other.

Hamilton is similar to Nakamura in that Hamilton teaches (see figures 1 and 2) transmitting an encrypted image (28) obtained from a camera (20) via a network (see paragraphs 0055-0056). Hamilton also similarly teaches of decrypting the image at a receiving device using a decryption key (paragraph 0057).

However, in addition to the teachings of Nakamura, Hamilton teaches that each camera has an identifier, and that said identifier is a unique identifying number (serial number, 22, figure 1). Hamilton also teaches a removable recording medium for recording said decryption key and the identifying number of said image pickup apparatus in association with each other (The key(20) and the serial number(22) may

be communicated from the retailer or manufacturer(i.e. the key generating apparatus) to an authorization center (i.e. image receiving device) by traditional hard copy methods (i.e. via a removable recording medium), paragraph 0079.). Hamilton also teaches that the image receiving device ("authorization center") is connected with the recording medium (The authorization center can receive a "hard copy" of the key, paragraph 0079. This key is used for image decryption, paragraph 0057. Because the key is in hard copy form, it would have to be connected with the image receiving device.).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to have the camera taught by Nakamura comprise a unique identifying number as taught by Hamilton, and have the decryption key taught by Nakamura recorded on a recording medium as taught by Hamilton for the benefit of ensuring that the images obtained at the viewer are images from the specific image capture device (Hamilton, paragraph 0005).

However, the combination of Nakamura and Hamilton does not explicitly teach an authenticating server for authenticating said image pickup apparatus accessible from said viewing apparatus.

Read is similar to Nakamura and Hamilton in that Read teaches an image transmission system (figure 1) for transmitting an image via a network (internet, 102), said image transmission system (figure 1) comprising one or a plurality of image pickup apparatus (104) each having a unique identifier (Cameras have unique identifiers so that a user can be permitted to or restricted from viewing certain cameras, paragraph 0036.).

However, in addition to the teachings of Nakamura and Hamilton, Read teaches an authenticating server (central server, 108) for authenticating said image pickup apparatus accessible from a viewing apparatus (The authenticating server (108) is accessible from a viewing apparatus (110, figure 1), and uses log-in/password security functions to authenticate that an image pickup apparatus is accessible by a viewing apparatus, paragraph 0024. If the viewer is authorized, then images received from the image capture device are immediately forwarded to the viewer, paragraph 0033.).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to include an authenticating server as taught by Read in the image transmission system taught by the combination of Nakamura and Hamilton for the benefit of increasing security.

Consider claim 3, Nakamura teaches:

An image transmission system for transmitting an image via a network (see figures 1A and 1B), said image transmission system comprising:

one image pickup apparatus (first terminal, 1, camera, 106a);

a transmitting apparatus (first terminal, 1) for encrypting an image picked up by said image pickup apparatus and transmitting the image to said network (The first terminal (1) is used for encrypting and transmitting real-time communication type information along a transmission path (3), column 4, lines 3-8. The image pickup apparatus includes a camera (106a) for picking up images for transmission, column 1,

lines 5-9, column 4, lines 29-32. The images are transmitted in "an on-line manner", column 5, lines 40-52.);

a key generating apparatus for generating, for each said image pickup apparatus, an encryption key for encrypting said image and a decryption key for decrypting said encrypted image (Images are encrypted in the image pickup apparatus (1) and decrypted in a viewing apparatus (2) using a generated "secret key", column 6, lines 11-16, lines 37-40. The encryption key is stored in a magnetic storage device (101) in the image pickup apparatus (1), column 6, lines 47-54, and transmitted to the viewing apparatus (2), column 9, lines 14-29. The secret keys are used to configure random number generators (109, 209) for encryption and decryption.); and

a viewing apparatus (second terminal, 2), having a decrypting function for decrypting said encrypted image using said decryption key, for communicating with said image pickup device, and for viewing the image transmitted via said network from said image pickup apparatus to said viewing apparatus (The viewing apparatus (2) comprises a CRT (206a) for displaying received image data, column 4, lines 61-66. Images are decrypted in a viewing apparatus (2) using a generated "secret key", column 6, lines 11-16, lines 37-40. The viewing apparatus (2) communicates with the image pickup apparatus (1) by requesting image data, column 6, lines 7-16. The viewing apparatus (2) decrypts encrypted image data using a key that is the same as the encryption key, which key is received from the image pickup apparatus, column 6, lines 47-69, column 9, lines 14-54.).

However, Nakamura does not explicitly teach that each image pickup device has a unique identifying number, or of a removable recording medium for recording said decryption key and the identifying number of said image pickup apparatus in association with each other.

Hamilton is similar to Nakamura in that Hamilton teaches (see figures 1 and 2) transmitting an encrypted image (28) obtained from a camera (20) via a network (see paragraphs 0055-0056). Hamilton also similarly teaches of decrypting the image at a receiving device using a decryption key (paragraph 0057).

However, in addition to the teachings of Nakamura, Hamilton teaches that each camera has an identifier, and that said identifier is a unique identifying number (serial number, 22, figure 1). Hamilton also teaches a removable recording medium for recording said decryption key and the identifying number of said image pickup apparatus in association with each other (The key(20) and the serial number(22) may be communicated from the retailer or manufacturer(i.e. the key generating apparatus) to an authorization center (i.e. image receiving device) by traditional hard copy methods (i.e. via a removable recording medium), paragraph 0079.). Hamilton also teaches that the image receiving device ("authorization center") is connected with the recording medium (The authorization center can receive a "hard copy" of the key, paragraph 0079. This key is used for image decryption, paragraph 0057. Because the key is in hard copy form, it would have to be connected with the image receiving device.).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to have the camera taught by Nakamura comprise a unique

identifying number as taught by Hamilton, and have the decryption key taught by Nakamura recorded on a recording medium as taught by Hamilton for the benefit of ensuring that the images obtained at the viewer are images from the specific image capture device (Hamilton, paragraph 0005).

However, the combination of Nakamura and Hamilton does not explicitly teach an authenticating server for authenticating said image pickup apparatus accessible from said viewing apparatus.

Read is similar to Nakamura and Hamilton in that Read teaches an image transmission system (figure 1) for transmitting an image via a network (internet, 102), said image transmission system (figure 1) comprising one or a plurality of image pickup apparatus (104) each having a unique identifier (Cameras have unique identifiers so that a user can be permitted to or restricted from viewing certain cameras, paragraph 0036.).

However, in addition to the teachings of Nakamura and Hamilton, Read teaches an authenticating server (central server, 108) for authenticating said image pickup apparatus accessible from a viewing apparatus (The authenticating server (108) is accessible from a viewing apparatus (110, figure 1), and uses log-in/password security functions to authenticate that an image pickup apparatus is accessible by a viewing apparatus, paragraph 0024. If the viewer is authorized, then images received from the image capture device are immediately forwarded to the viewer, paragraph 0033.).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to include an authenticating server as taught by Read in the

image transmission system taught by the combination of Nakamura and Hamilton for the benefit of increasing security.

13. Claims 14-17 and 22-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hamilton(US 2002/0118837) in view of Read(US 2004/0066456).

Consider claim 14, Hamilton teaches:

A key generating apparatus for generating an encryption key used for encryption processing in transmitting an image(27) via a network(See paragraph 0058, figures 1 and 2. A key(22) is generated by a retailer or manufacturer and stored in a camera(12). The key is used to encrypt images, paragraph 0047. A pseudo-random number generator may be used to generate keys, paragraph 0068.), and a decryption key(paragraph 0071),

wherein said key generating apparatus generates the encryption key(20) for encrypting said image(27) and transmits the encryption key(20) to an image pickup apparatus(12) having a unique identifying number(serial number, 22) and having an encrypting function for encrypting a picked-up image for transmission over the network(paragraphs 0055-0056); and

said key generating apparatus generates the decryption key for decrypting said encrypted image and transmits the decryption key to a removable recording medium for recording said decryption key and the identifying number of said image pickup-apparatus in association with each other(The key(20) and the serial number(22) may be

communicated from the retailer or manufacturer(i.e. the key generating apparatus) to an authorization center by traditional hard copy methods(i.e. via a removable recording medium), paragraph 0079. The key(20) allows the decryption of images taken by the camera, paragraph 0071.).

Hamilton does not explicitly teach that the image is transmitted from the camera to a viewing apparatus.

Read is similar to Hamilton in that Read teaches an image transmission system(figure 1) for transmitting an image via a network(internet, 102), said image transmission system(figure 1) comprising one or a plurality of image pickup apparatus(104) each having a unique identifier(Cameras have unique identifiers so that a user can be permitted to or restricted from viewing certain cameras, paragraph 0036.).

However, in addition to the teachings of Hamilton, Read teaches that a viewer is authenticated by an authentication server and is permitted to receive encrypted images from the image pickup apparatus(An authenticating server(108) is part of a viewing apparatus(108, 110). It authenticates which cameras a user is authorized to view via a user-ID/password, paragraphs 0035-0037. The viewing apparatus comprises display elements such as laptops and cellular telephones, paragraph 0021. The viewing apparatus(108) decrypts the image data for display, paragraph 0044.).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to include a secure viewing apparatus as taught by Read in the network taught by Hamilton for the benefit of improving the versatility of the system

by enabling an authorized user to view remotely captured image data (Read, paragraph 0005).

Consider claim 15, and as applied to claim 14 above, Hamilton further teaches that said key generating apparatus has a linking function for linking said image pickup device(12) to said network(Hamilton teaches that the keys can alternatively be generated in an authorization center(14), paragraphs 0068 and 0078. Images(27) are sent to the authorization center(14) from the camera(12), paragraph 0056. The authorization center(14) may then communicate images(27) to a verifying entity(16). Therefore, the authorization center(i.e. key generating apparatus) links the image pickup device to the overall network.).

Consider claim 16, and as applied to claim 14 above, Hamilton teaches that keys are generated by an external source(see claim 14 rationale). Hamilton does not explicitly teach that said key generating apparatus has a compressing function for compressing the image picked up by said image pickup apparatus.

However, in addition to the teachings of Hamilton, Read teaches that the key generating apparatus(106) is in a personal computer(paragraph 0026) connected to a plurality of cameras(104, figure 1), and that the key generation apparatus(106) compresses the image data(paragraph 0026).

Consider claim 17, and as applied to claim 14 above, Hamilton further teaches a computer program stored on a computer readable medium, for making a computer function as the key generator of claim 14(See paragraphs 0068. A pseudo random number generator generates keys of desired lengths, such as 128-bits. A computer program stored on a computer readable medium would have to be used to enable the operation and key generation of the pseudo-random number.).

Consider claim 22, Hamilton teaches:

An image pickup apparatus(12, figures 1 and 2) used in an image transmission system(figure 1) for transmitting an image(28) via a network(paragraph 0056), said image pickup apparatus(12) comprising:

a recording unit(22) for recording a unique identifying number(serial number, paragraph 0048);

an encrypting unit for encrypting a picked-up image(paragraph 0055); and

a communicating unit(23, paragraph 0049, not shown in drawings) for transmitting said encrypted image to a viewer(verifying entity, 16, paragraphs 0056-0057).

However, Hamilton does not explicitly teach that the viewer has been authenticated by an authentication server and is permitted to receive encrypted images from the image pickup apparatus.

Read is similar to Hamilton in that Read teaches an image transmission system(figure 1) for transmitting an image via a network(internet, 102), said image

transmission system(figure 1) comprising one or a plurality of image pickup apparatus(104) each having a unique identifier(Cameras have unique identifiers so that a user can be permitted to or restricted from viewing certain cameras, paragraph 0036.).

However, in addition to the teachings of Hamilton, Read teaches that the viewer has been authenticated by an authentication server and is permitted to receive encrypted images from the image pickup apparatus(An authenticating server(108) is part of a viewing apparatus(108, 110). It authenticates which cameras a user is authorized to view via a user-ID/password, paragraphs 0035-0037.).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to include an authenticating server as taught by Read to permit or prohibit viewers from receiving the encrypted images taught by Hamilton for the benefit of improving security by only allowing viewers access to authorized and appropriate images.

Consider claim 23, and as applied to claim 22 above, Hamilton further teaches that said communicating unit includes a receiving unit for receiving an encryption key for encrypting said image from a key generating apparatus(paragraphs 0058, 0068 and 0078).

Consider claim 24, and as applied to claim 22 above, Hamilton further teaches that said communicating unit includes at least one of a USB port(see paragraph 0049).

Allowable Subject Matter

14. Claims 18-21 are objected to because of the informalities indicated in paragraphs 6-8 above, but would be allowable if correction is made.

15. The following is a statement of reasons for the indication of allowable subject matter:

Consider claim 18, the prior art of record teaches a computer program, stored on a computer readable medium for making a computer initialize an image transmission system, authenticate a user and image pickup apparatus, connect the image pickup apparatus to a viewing apparatus, identify the image pickup apparatus via an identification number, obtain a decryption key, transmit an image request, receive an image subsequent to the image transmit request, decrypt the image, and display the image on a viewing apparatus.

However, the prior art of record does not teach nor reasonably suggest, as a whole, that the initializing of the image transmission system comprises connecting an image pickup apparatus and a memory card to a key generating apparatus, transmitting an identifying number from the image pickup apparatus to the key generating apparatus, registering the identifying number from the image pickup apparatus at the key generating apparatus and at an authentication server; and generating an encryption and decryption key unique to the image pickup apparatus.

Claims 19 is allowed as depending from an allowed claim 18.

Consider claim 20, the prior art of record teaches an image transmission system for transmitting an image via a network comprising an image pickup apparatus connected to a key generating apparatus comprising a recording unit for storing an identifying number and an encryption key from the key generating apparatus, an image viewer with an interface for requesting authentication by an authentication server of an image capture apparatus accessible by a user, connecting the image pickup apparatus to the viewing apparatus, a memory for obtaining a decryption key from the removable storage medium, a decrypting unit for decrypting receiving images, and a display for displaying the decrypted images.

However, the prior art of record does not teach nor reasonably suggest, as a whole, that the key generating apparatus comprises a network interface for registering the identifying number from the image pickup apparatus at an authentication server, a recording unit for storing the the-identifying number from the image pickup apparatus, an encryption key generation unit for generating an encryption and decryption key unique to the image pickup apparatus, and an interface for storing the decryption key in a removable storage medium.

Claim 21 is allowed as depending from an allowed claim 20.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ALBERT H. CUTLER whose telephone number is (571)270-1460. The examiner can normally be reached on Mon-Thu (9:00-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ngoc-Yen Vu can be reached on (571) 272-7320. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/AC/
10/04/2008

/Ngoc-Yen T. VU/
Supervisory Patent Examiner, Art Unit 2622

.